# Sistemas Distribuídos, 2017/18 - 2º MINI Teste

Todas as perguntas têm a mesma cotação. Escolha apenas uma resposta em cada alínea.
Cada resposta de escolha múltipla errada desconta 1/4 da sua cotação.
**No caso de encontrar mais do que uma resposta certa, escolha a que faz a afirmação mais forte.**

## Número: _____ Nome:_____

1) Com a cifra assimétrica RSA é possível:
   A) Cifrar com a chave pública, decifrar com a chave privada.
   B) Cifrar com a chave privada, decifrar com a chave pública.
   C) Combinar com função de resumo para construir assinaturas digitais.
   D) Todas as anteriores.

2) Um certificado digital de chave pública confiável deve conter, pelo menos:
   A) A chave pública da entidade.
   B) A chave pública e o nome da entidade certificada.
   C) O par de chaves da entidade certificada.
   D) A chave pública, o nome da entidade certificada e a assinatura de uma autoridade de certificação.

3) Considere uma entidade A cujo par de chaves de cifra assimétrica foi criado pela entidade certificadora CA. Verificou-se que a entidade não é confiável e lhe deveria ser inibido o uso do certificado.
   A) A CA invalida o certificado e deixa de responder a pedidos do certificado de A.
   B) A CA muda a sua chave pública para que o certificado deixe de ser válido.
   C) O certificado da entidade A deve ser acrescentado à CRL da CA.
   D) A CA informa os detentores de certificados que já não são válidos.

4) A Andreia e o Benjamim não se conhecem mas pretendem comunicar entre si através de uma rede insegura. Para o protocolo de segurança vão recorrer à cifra assimétrica RSA. O Benjamim envia uma mensagem à Andreia (B->A) e ela depois responde com outra mensagem (A->B):

   B->A: $K_{pub}B$
   A->B: $\{M\}K_{pub}B$
   onde: M é a mensagem, {} representa cifra

   Para que a Andreia possa ter a certeza que apenas o Benjamim vai ler a mensagem:

   A. Não é necessário mais nada.
   B. É necessário acrescentar $\{D(K_{pub}B)\}K_{priv}T$ à primeira mensagem (B->A), e assumir que o Tomás conhece as chaves públicas da Andreia e do Benjamim.
   C. É necessário acrescentar um certificado digital de chave pública de $K_{pub}B$ assinado por uma autoridade de certificação (Tomás) na qual a Andreia e o Benjamim confiam.
   D. B ou C, desde que a Andreia e o Benjamim conheçam previamente $K_{pub}T$

5) Pretende-se garantir **integridade** e **confidencialidade** de uma mensagem M que vai ser transmitida numa rede insegura. Existe uma chave simétrica K partilhada pelo emissor e recetor. Estão disponíveis as seguintes funções criptográficas: CifraAES, CifraDES, DecifraAES, DecifraDES, SHA2, HmacSHA2, MD5, HmacMD5.
O que se deve enviar?
A. CifraAES(M, SHA2(K))
B. CifraAES(M, K), HmacSHA2(M, K).
C. M, HmacSHA2(M, K)
D. CifraDES(M, K), HmacMD5(M, K).

6) Um cliente a executar uma transação distribuída chamou a operação closeTransaction(true) para que a transação seja confirmada. Numa situação sem falhas nem atrasos, no momento da chamada, a primeira ação feita pelo coordenador será:
A) Enviar a mensagem canCommit a cada participante.
B) Enviar a mensagem doCommit a cada participante.
C) Enviar o seu voto aos participantes.
D) Confirmar localmente a transação.

7) O 2-phase commit baseia-se no uso de *timeouts*.
A) Consequentemente, o protocolo só pode ser usado em sistemas síncronos.
B) Consequentemente, o protocolo exige relógios sincronizados.
C) Apesar de usar *timeouts*, o protocolo pode ser usado em sistemas assíncronos.
D) Nenhuma das anteriores.

8) No 2-phase commit, o Coordenador recebeu voto NÃO de um dos participantes.
A) Escusa de esperar por outros votos; pode enviar imediatamente a ordem de doAbort a todos os participantes.
B) Escusa de esperar por outros votos; pode enviar imediatamente a ordem de doCommit a todos os participantes.
C) Espera pelos votos dos participantes em falta e só depois envia doAbort a todos.
D) Espera pelos votos dos participantes em falta e só depois envia doCommit a todos.

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | **Total** |
|---|---|---|---|---|---|---|---|---|
| 2,5 | 2,5 | 2,5 | 2,5 | 2,5 | 2,5 | 2,5 | 2,5 | **20** |
| D | D | C | D | B | A | C | A | |